AMENDMENTS TO THE SPECIFICATION

Please replace the paragraphs found on page 4 line 28 to page 6 line 9 with the following:

Client devices ~~102~~101-104 may be configured as public systems, such as kiosks, home computing devices, personal computing devices, personal mobile computing device, and the like, that are used by an employee, or the like, of the enterprise to access an enterprise resource, such as resource server 110. Such client devices may not be issued or maintained by the enterprise, typically resulting in a classification as an untrusted device.

Similarly, client devices ~~102~~101-104 may be maintained, issued, and configured by a business partner, and the like. These client devices may also be classified as untrusted devices. Such client devices may be employed by such nonemployees to the enterprise to seek access to an enterprise resource, for example, to share a file, obtain extranet access, and a similar limited resource.

Client devices ~~102~~101-104 may also be configured, maintained, and issued by the enterprise to an employee, and the like, of the enterprise. Such client devices may be considered to be trusted devices.

The invention is not limited, however, to a binary level of trust. Degrees of trust may also be employed to describe client devices ~~102~~101-104. For example, a personal laptop may be considered to have a higher level of trust than a kiosk. Similarly, an enterprise maintained and issued laptop may have a higher level of trust than the personal laptop, but a lower level of trust than an enterprise desktop.

Client devices ~~102~~101-104 typically include a browser application, and the like, that is configured to enable network access through firewall 106 to communicate with RPM 108. Client devices ~~102~~101-104 may be further configured to enable a secure communication with RPM 108 using such mechanisms as Secure Sockets Layer (SSL), IPSec, Tunnel Layer Security (TLS), and

the like. In one embodiment, client devices ~~102~~101-104 are configured to establish a communication with RPM 108 employing an IPSec VPN.

Client devices ~~102~~101-104 may further include a client application, and the like, that is configured to manage various actions.

Network 105 is configured to couple client devices ~~102~~101-104, and the like, with resource server 110 through firewall 106 and RPM 108. Network 105 is enabled to employ any form of computer readable media for communicating information from one electronic device to another. Also, network 105 can include the Internet in addition to local area networks (LANs), wide area networks (WANs), direct connections, such as through a universal serial bus (USB) port, other forms of computer-readable media, or any combination thereof. On an interconnected set of LANs, including those based on differing architectures and protocols, a router may act as a link between LANs, to enable messages to be sent from one to another. Also, 5 communication links within LANs typically include twisted wire pair or coaxial cable, while communication links between networks may utilize analog telephone lines, full or fractional dedicated digital lines including Tl, T2, T3, and T4, Integrated Services Digital Networks (ISDNs), Digital Subscriber Lines (DSLs), wireless links including satellite links, or other communications links known to those skilled in the art.

Please replace the paragraph found on page 6 lines 19-23 with the following:

Furthermore, remote computers and other related electronic devices could be remotely connected to either LANs or WANs via a modem and temporary telephone link. In essence, network 105 includes any communication method by which information may travel between client devices ~~102~~101-104 and firewall 106 to RPM 108, resource server 110, and the like.

Please replace the paragraph found on page 8 lines 18-24 with the following:

Resource server 110 represents virtually any resource service, device, and the like, to which client devices ~~102~~101-104 may seek access. Such resources may include, but is not limited

to, web services, mail services, database services, repositories, legacy services, telnet services, FTP services, and the like. As such resource server 110 may be implemented on a variety of computing devices including personal computers, desktop computers, multiprocessor systems, microprocessor-based devices, network PCs, servers, and the like.

Please replace the paragraph found on page 12 lines 8-16 with the following:

In one embodiment, network device 200 includes one or more Application Specific Integrated Circuit (ASIC) chips (not shown) connected to bus 222. In one embodiment, network interface unit 210 may connect to the bus through the ASIC chip. The ASIC chip may include logic that performs some of the functions of network device 200. For example, in one embodiment, the ASIC chip performs a number of packet processing functions, to process incoming data, apply a policy based on the received data, and based on the policy configure access to a resource, configure a connection between the resource and a client device, apply a virtual sandbox 116 to the client device, its connection, and the like.

Please replace the paragraph found on page 12 lines 24-30 with the following:

The operation of certain aspects of the invention will now be described with respect to FIGURES 3-4. FIGURE 3 illustrates a logical flow diagram generally showing one embodiment of a process for managing access to a resource based on a dynamic policy. Process 300 of FIGURE 1 may be implemented within RPM 108 of FIGURE 1. Process 300 typically is entered when a remote client device such as one of client devices ~~102~~101-104 of FIGURE 1 seeks access to a network resource protected by the invention.

Please replace the paragraphs found on page 13 lines 1-26 with the following:

Process 300 begins, after a start block, at decision block 302, where a determination is made whether a component, such as a control, application, script, or the like, may be downloaded onto the remote client device seeking access to the network resource. The component may not be downloadable for a variety of reasons, including, the client device is not able to receive and/or

execute the component, the client device has been configured to not accept downloads, and the like. In any event, if it is determined that the component may not be downloaded to the client device, processing branches to block 308; otherwise, process proceeds to block 304, where the component is downloaded onto the client device. The downloaded component may include one or more additional components, including another control, application, script, and the like, configured to inspect the environment associated with the client device, enable a virtual sandbox 116 associated with the client device, and the like. The other downloaded component may also be employed to provide client device cleanup upon session termination, as further described below in conjunction with FIGURE 4.

Process 300 proceeds next to block 306, where the downloaded component(s) analyzes the environment associated with the client device. Analysis may include, but is not limited to, determining such information as how the client device is configured, whether it is a trusted or untrusted device, type of encryption enabled on the client device, type of antivirus enabled on the client device, other security features that may be enabled on the client device, and the like. Analysis may also include determining the browser type and version, operating system, including version and patch level, enabled and available security certificates, and the like. Analysis may further include determining whether a hacker tool 114 is enabled on the client device, such as a network sniffer, a screen scraper, a password cracker, or the like. The presence of an enabled hacker tool 114 may indicate an attempt that the client device is not to be untrusted. In any event, the determined information is sent back to a policy manager.

Please replace the paragraphs found on page 14 lines 16 to page 15 line 28 with the following:

Process 300 proceeds next to block 314 where the connection between the client device and the requested resource is configured. The connection may be configured to restrict selected actions, operations, downloads, and the like. Such restrictions may include, but are not limited to, restricting access to a predetermined application, access to a predetermined file, group of files, folders, services, servers, and the like. For example, in one embodiment the connection may be

configured to include a virtual sandbox 116 which may restrict a client device from performing certain actions.

The virtual sandbox 116 may include configuring the client device to prevent one or more actions on certain documents, files, and the like. In one embodiment, the virtual sandbox 116 is configured to intercept selected system actions to prevent their completion. For example, the virtual sandbox 116 may disable system actions such as a save command, a print command, a move command, a copy command, other I/O messages, and the like. For example, the virtual sandbox 116 may prevent a save command from saving data to a file, creating a new file, and the like. Similarly, the virtual sandbox 116 may prevent the move command from enabling a move of a file, folder, or the like, from one location to another, including, but not limited to, from one computing device to another computing device. Additionally, the virtual sandbox 116 may restrict the client device from sending an email message, or the like.

The virtual sandbox 116 may also restrict the client device from launching predetermined applications, such as a mail-client, FTP application, and the like.

The virtual sandbox 116 may be implemented employing a variety of mechanisms. For example, the virtual sandbox 116 may include a downloaded component where permitted. The virtual sandbox 116 may also include an interface component arranged to intercept the communications between the client device and the requested resource. The virtual sandbox 116 may then intercept commands, files, and the like, between the requested resource and the client device to restrict transmission of selected requests, files, commands, instructions, data, results, and the like. The virtual sandbox 116 may also send instructions to applications on the client device to selectively restrict actions, disable operations, and the like. For example, the virtual sandbox 116 may send an instruction to the client browser to direct the browser not to save files, documents, and the like.

The virtual sandbox 116 may also redirect access to documents, files, and the like, to a location, remote from the client device. For example, the virtual sandbox 116 may redirect an

instruction intended to access a local cache, a bookmark, and the like, on the client device to instead seek access to a location, bookmark, and the like, on a remote server, or the like. In another embodiment, the virtual sandbox 116 may make it appear that the client's browser is writing to or reading from a local location on the client device, even though it is actually writing to or reading from a remote server location.

The virtual sandbox 116 may also direct actions on the client device to encrypt selected files on the client device, employing an encryption key that may reside at a remote server location, employing a key in volatile memory, or the like. In this manner, should a connection be terminated with the resource, the client device loses power, or the like, the files on the client device remain encrypted.